
梆梆安全
BANGCLE
2016物联网安全白皮书
梆梆安全研究院

前言

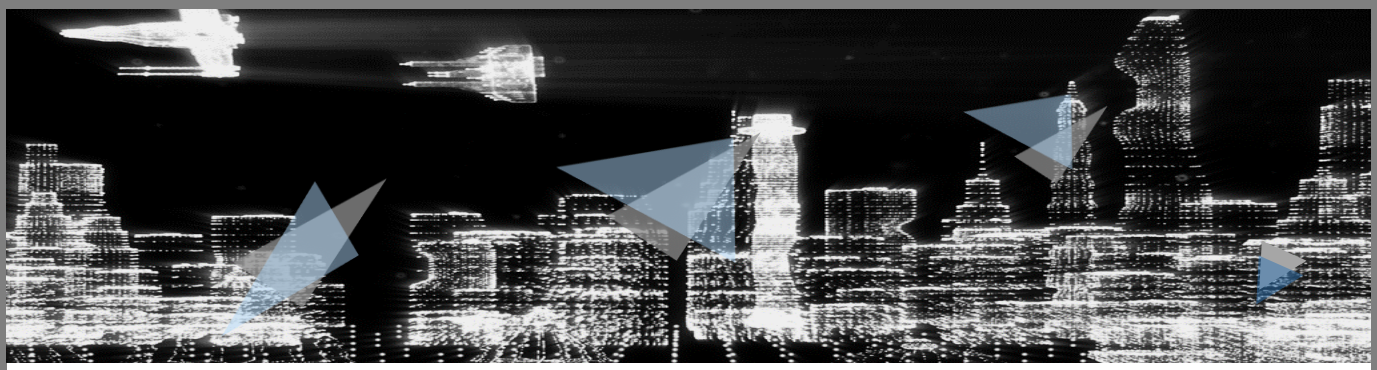
物联网被人们视为继计算机、互联网之后信息技术产业发展的第三次革命，其泛在化的网络特性使得万物互联正在成为可能。智能家居、车联网、人工智能……这一切的背后正是物联网在加速落地、快速成熟，物联网时代的到来已经毋庸置疑。

物联网的基础与核心仍然是互联网，其是在互联网基础上的延伸与拓展，而云计算、移动互联网、智能移动终端等则在帮助物联网的体系架构变得愈发丰富饱满。然而，正是由于物联网络对于互联网络的天然继承性，使得针对互联网所发起的各类恶意攻击开始蔓延到了物联网领域。

互联网在被创造伊始并未将“安全”作为首要考量因素，这使其在诞生之初就存在“安全免疫缺陷”。继承于互联网的物联网，不仅融合了互联网的长处与优势，同时也天然携带了这份“安全免疫缺陷”基因，加之物联网自身不断展现出来的新特性，使得这一安全缺陷在被持续扩大化。

如今，各类智能可穿戴设备、智能汽车、智能交通、智慧医疗……都在依托于物联网，它们或是物联网的感知终端，或是物联网中的一个分支生态环境。物联网的构成元素很小，小到一个芯片；物联网的构成元素也很大，人工智能体的“骨架”与“神经”就是一套物联网系统单元。所以，物联网是一个标准的“简单”与“复杂”混合体，这直接导致其所面临的安全问题非常“麻烦”。

最好的安全，就是能够直指事物本质的安全，物联网安全尤需如此。



物联网应用特征决定物联网安全本质

物联网有着不可计数的感知终端，有着复杂的信息通讯渠道，有着庞大的数据存储与处理中心。但抽象来看，物联网正是一个十分标准的“终端——传输管道——云端”架构。

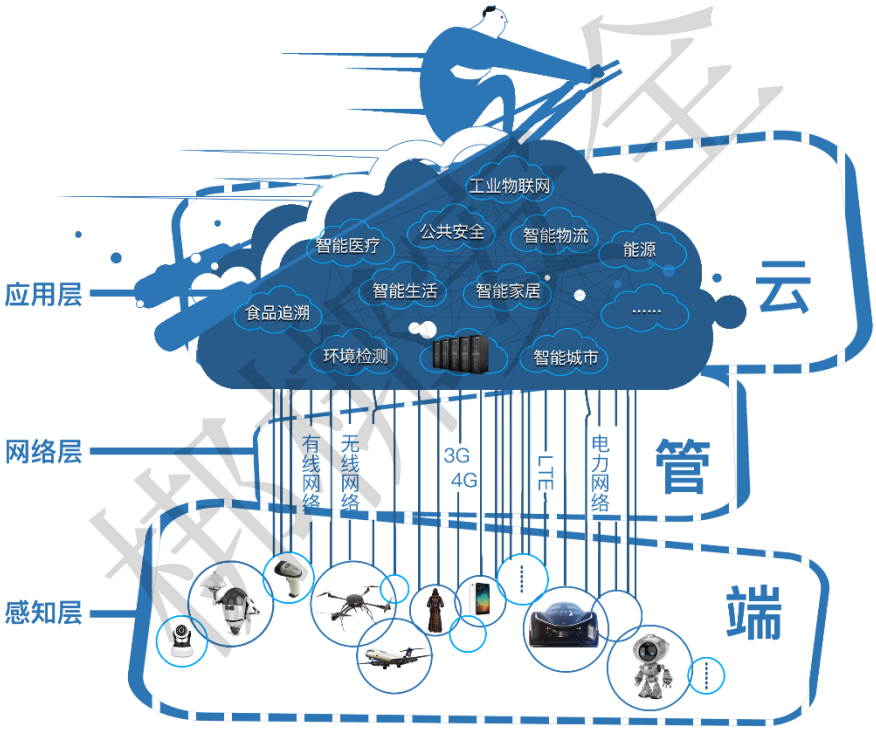
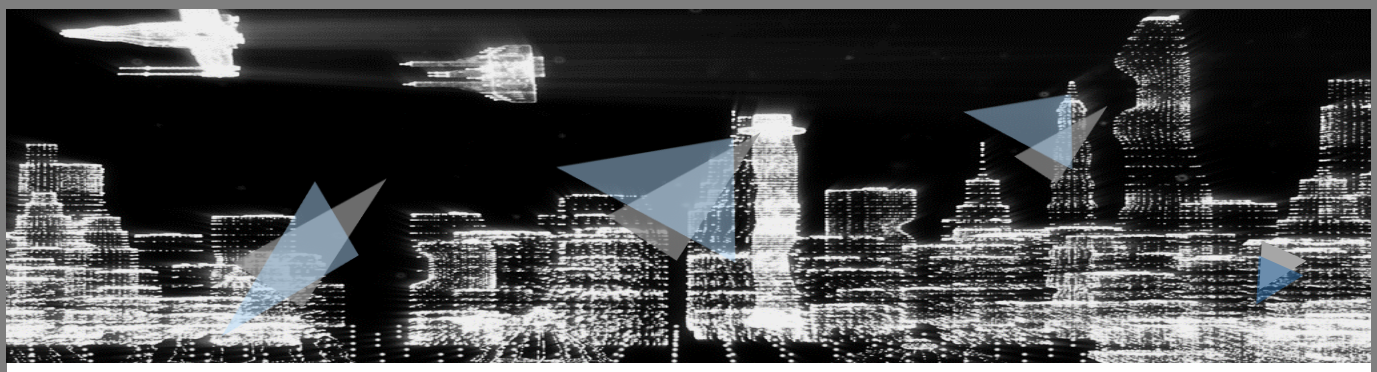


图 物联网“端-管-云”架构

与计算机时代、网络时代相比较，物联网的终端具有移动化、微型化等特征，其传输管道更是在有线网络之外又增加了无线网络，物联网的云端数据中心不仅更大也更为灵活。物联网体系架构里可编程、可通讯、智能化、网络化的特征要素愈发凸显，而物联网所面临的特殊安全挑战也由此而生，即所谓的：代码之殇、联网之疫、攻防之悖。

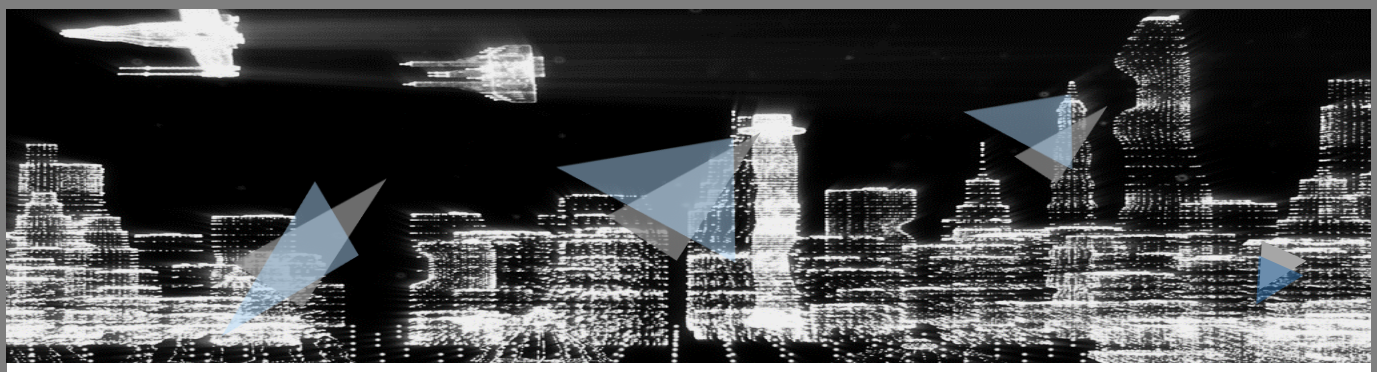


代码之殇：从计算机诞生那一刻起，与之相依存的代码程序就一直在软件层面推动着信息产业的发展与变革。而作为代码与生俱来的“漏洞”，则成为了诱发各类安全问题的关键所在。数据显示，软件行业平均每1000行代码中约有30个漏洞，而Linux内核每10000行代码里则有1-5个漏洞。如今的车载信息娱乐系统，其软件代码很容易超过1亿行，而无人驾驶系统的代码量更会达到甚至超过2亿行以上。极其复杂系统的背后，潜藏的是数量繁多的未知安全漏洞。这也直接导致，代码安全漏洞依然是物联网时代黑客对智能设备发起攻击的聚焦点。例如，通过对智能设备固件内部的代码进行挖掘分析，找到加密方法和密钥，就能够知道消息会话的内容（账号密码、隐私信息、机密数据等等）。

联网之疫：随着智能设备纷纷接入互联网络，为人们提供了更为多元化、全面的服务，但在这些设备所打开诸多对外连接接口的背后，危机已然降临！2020年全球联网设备将可能达到260亿，也就是说未来会有更多的设备与基础设施需要进行网络互联。联网越多，被打开的接口就越多，黑客可以利用的攻击面就越大。

当年著名的震网病毒（Stuxnet）还是利用移动介质进入物理隔离的工业控制网络，通过操控PLC数据导致伊朗纳坦兹浓缩铀工厂约20%的离心机失控、报废。而今年，震惊全球的美国断网事件，却仅仅是黑客通过操控网络摄像头及相关DVR录像机发起物联网DDoS攻击测试所导致的。一时间，Twitter、Paypal、Spotify、Netflix、Airbnb、Github、Reddit以及纽约时报等美国知名网站皆无法访问，满屏都是“404错误”。

网站、业务服务器、邮件系统、用户数据、带宽……物联网时代，黑客的可攻击面在变得愈加广泛，网络攻击几乎时刻都在发生。监测发现，国内应用商店中Top 100的App（移动应用）100%都遭受过严重攻击。早期的智能终端设备虽然未采取基本安全防护措施，但由于不与外界连接，处于隔离环境，所以没有显露出安全风险。



现在网络连接的打通，让这些设备毫无防备地暴露在网络安全“疫区”里。以这些不设防的智能终端设备为攻击跳板，黑客们将能够更为轻松地篡取藏身于其后的巨大经济利益。

攻防之悖：智能设备价格上的“优势”，意味着任何人都可以购买智能设备，并进行破解、阻止升级等操作尝试；意味着所有智能设备都可能遭受白盒攻击，运行在一个完全被控制的环境中；意味着智能设备的所有者可能就是攻击者。

黑客可以通过充电桩、道路交通牌、手机App对智能汽车进行入侵攻击，还可以透过可穿戴设备里的移动支付功能潜入被严密防护的银行后台系统。复杂的物联网系统架构，使得黑客仅需要攻击整个生态系统里最不起眼、最为薄弱的一环，就可以借助“蝴蝶效应”实现对目标的最终破坏。如今的安全防护都是基于现有技术，但快速发展的智能设备却需要防御未来新的攻击方法与工具。以现在安全机制防御未来攻击，这个悖论正如紧箍咒般套在物联网的头上。

物联网安全本质：透过表象可以发现，所有安全威胁与黑客攻击最终都是利用程序中的脆弱性实现入侵以获得控制权，因此代码安全是最本质、最核心的关键问题。那么物联网体系的安全就需要回归本质，通过保护代码来强健物联网自体。另外，还需要考虑通过微边界防御打造多重安全机制，提升物联网免疫能力，建设端管云泛在化安全架构，构筑智能生态安全。

物联网安全方法论

传统安全解决方案面对接入网络的新型智能设备以及针对智能设备的新兴恶意攻击缺少有效保护方案与应对策略，因此物联网安全需要考虑特殊的解决方法：要做到安全入微，更要实现统筹安全、度量安全。

每个智能设备都是物联网中的一个微点，会受到各种攻击。这些微点极小又极多，而且脱离了传统安全防御的范畴。考虑到有些微点里可能仅有几K字节的运行代码，这就需要对微点的安全防护做到极轻，以轻量级的安全防护保障微点的正常运转。然后通过构造多层次、多样性保护系统，使得微点拥有足够强度的安全防护及抗攻击能力。进而让安全能力泛在化物联网的每个环节、每个角落，从全生态系统、全生命周期维度对物联网体系安全进行考虑与规划，做到物联网安全极大化。最为关键的是要逐步建立起物联网安全度量方法与规范，并据此设立物联网安全基线，由此让繁琐的物联网安全清晰可判断。

在这里尝试首次建立**物联网安全方法论：**

1、物联网安全要从设计阶段便予以考量，需要深入到代码层面；

2、赋予物联网端点智能安全能力，构建端点智能自组织安全防护循环微生态；

3、构筑极微安全防御体系，以细粒度安全防护叠加方式使得终端的轻量级安全拥有足够强度的抗攻击能力；

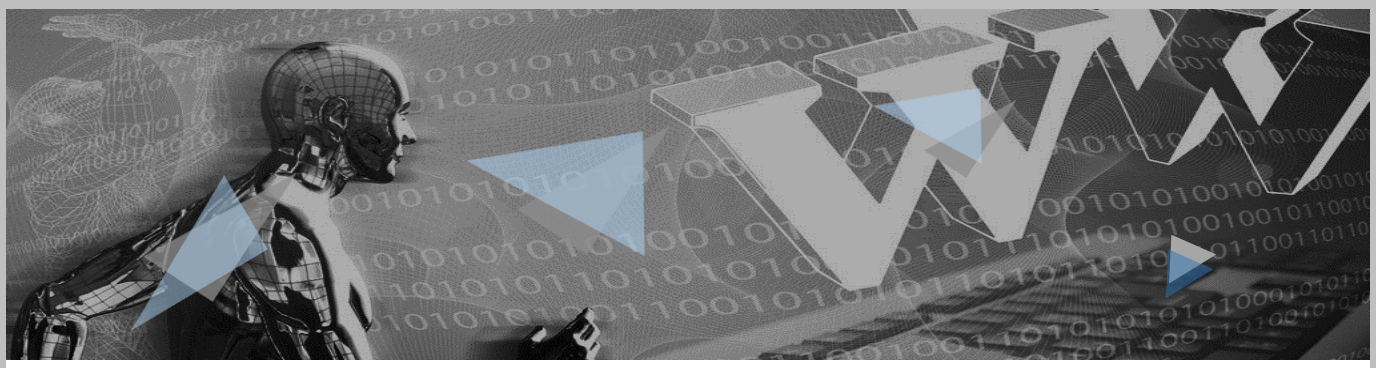
4、实现对终端立体防御体系内安全机制的即时动态聚合，运用整体力量对抗单点式恶意攻击；

5、物联网不仅需要使其安全能力可以实现在自身体系架构内部的全方位覆盖，同时还要延伸泛在化到物联网安全生态的各个维度中；

6、通过安全度量，为各个物联网安全系统设立恰当的安全基线；

7、耦合不同安全运维平台，实现对物联网整体安全的全面管控。

在一切事物本质背后所显露出来的就是正确的解决之道，透视恶意攻击表象，物联网世界安全防御的方法在愈加清晰——物联网安全需要渗透到“骨子”里。



化境入微的物联网终端安全

物联网的终端设备种类繁多，RFID芯片、读写扫描器、温度压力传感器、网络摄像头、智能可穿戴设备、无人飞机、智能空调、智能冰箱、智能汽车……体积从小到大，功能从简单到丰富，状态或联网或断开，唯一的共同之处就是天生都处于白盒攻击环境中。想要通过安装传统安全软件或者架设传统安全硬件的方式为其提供安全防护能力，明显行不通。

计算机时代，终端面临的最大安全威胁就是各类计算机病毒，防毒卡、杀毒软件等能够提供有效的安全防护。而网络时代，终端所面临的安全威胁剧增起来，木马、间谍软件、劫持攻击、钓鱼邮件、钓鱼网站等等。此时除了在终端上安装安全软件外，还需要在网络边界架设防火墙、IDS/IPS，在服务端进行系统加固、邮件过滤等更多的安全防御方法。

物联网时代许多终端的存储能力、计算能力都极为有限，在其上部署安全软件或者高复杂度的加解密算法都会大大增加终端运行负担，甚至导致终端无法正常运行。移动化更是使得传统网络边界“消失”，依托于网络边界的安全软、硬件产品都无法正常发挥作用。

而通过对典型物联网攻击案例分析可以发现，物联网时代攻击者主要瞄准的目标依然是物联网终端芯片里的智能设备“大脑”——代码。黑客在掌握了恰当的终端设备硬件平台、操作系统入侵方法后，就会设法对核心代码IP（算法）进行窃取，尝试破解密钥、加密算法，挖掘控制协议、后台交互逻辑漏洞，发现后台漏洞等等。进而实现暴露系统漏洞、对系统后台进行攻击（协议攻击）、控制系统、劫持/控制设备、获取用户信息/机密数据等操作。

综合考虑物联网终端自身特性，以及其所面临恶意威胁的特征，需要安全防护能力与物联网终端进行更加紧密地融合，需要在终端设备软硬件架构设计阶段即考虑安全性，需要安全防护能力能够深入到终端的代码层，需要安全防护能力能够尽可能地实现轻量化。

所以，对于终端的设计要遵循严谨的安全准则，对于终端里的代码程序，要想办法隐藏设计思路与细节，防止漏洞挖掘及恶意利用。其中一种解决办法就是对核心代码进行加密，在运行时解密，执行后清空内存，实现对代码的动态保护。而同态加密则强调数据在运行时依然保持加密状态，不给恶意攻击一丝可乘之机。

还有一种解决方案是对源代码进行混淆操作，通过插入冗余代码来隐蔽核心代码，进行等效变换保证输出执行结果的一致性，在代码重构后实行控制流的扁平化。多种技术手段相结合保护源码使其呈现多样性，让每次保护后的代码都不一样。在这种安全能力的防护下，黑客将对物联网终端里的代码无计可施，同时还不会消耗过多终端资源，影响终端业务的正常运行。

另外，还有一种新型对抗白盒攻击的技术——白盒密码技术，能够应用于物联网终端安全防护。白盒密码技术基于可逆的数学变换，将密钥隐藏在变换中，加解密运算中密钥不会出现在内存或者程序里。白盒密码技术可以支持多种算法，包括DES、3DES、AES、SM4、RSA等。借助白盒密码技术可以实现一设备一密钥，更可运行在嵌入式芯片里，保护核心密钥与数据。

虽然，物联网的移动化特性打破了传统的网络边界，但在每个终端微点之间实际上还是存在着一条新的无形边界——微边界，物联网领域攻防对抗的第一战场就是于微边界处展开。微边界上聚集着数以百万千万计的终端微点，一个感知终端的安全漏洞将会沿着微边界横向纵向扩展，并在物联网上被级数放大，由单个微点所最终导致的安全风险损失不可估量。

因此，要将安全泛在化于每个微边界点上，使每个终端微点都具备安全防护及抗攻击能力。安全的部署和运维也要能够适应海量并且多样化、多元化的感知设备。安全威胁的发现、监测与响应更要能够细粒度到每个微边界点上。

以上几种物联网终端安全技术，充分考虑到了物联网终端的物理特性，在不对终端施加过多负担的同时，使其拥有了足够的安全防护能力。

多重隔离的物联网通讯安全

数据通讯传输也是物联网体系里十分重要的一环，现在越来越多的黑客开始瞄准通讯传输协议下手进行破解攻击，加强数据通讯传输管道的安全性已经迫在眉睫。

意大利Sapienza大学的C.M.Medaglia和A.Serbanati在其所发表的论文《An overview of privacy and security issues in the internet of things》中曾指出，物联网终端在与云端进行信息通讯互动传输过程中，容易遭受流量分析、窃取、嗅探等网络攻击，进而导致传输信息数据遭遇泄露、劫持、被篡改（干扰）、屏蔽等威胁。

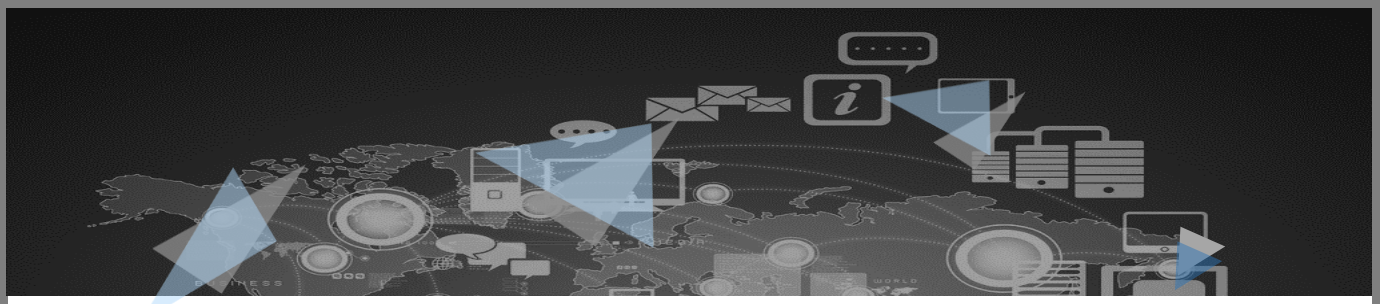
物联网数据传输所使用的网络包含有线网络、无线网络、3G、4G、LTE、电力载波等多种异构网络，其所面临的安全问题也很复杂。算法破解、协议破解、中间人攻击等诸多攻击方式正在逐渐侵蚀物联网体系，Key、协议、核心算法、证书等破解情况的发生，将会导致核心业务逻辑和重要接口暴露，甚至是更多不可预知的物联网系统性安全风险。但抽象来看，物联网数据通讯传输的安全问题需要重点关注传输管道自身与传输流量内容这两方面。

正如前文所提，已经有黑客通过分析、破解智能平衡车、无人机等物联网设备的通讯传输协议，实现了对物联网终端设备的入侵、劫持。网络通讯协议自身的安全性向来都不是很强，某些设备所采用的自定义网络通讯协议的安全性则更为堪忧。而在一些特殊物联网环境里，网络通讯过程中所传输的信息数据仅采用了很简单的加密办法，甚至没有采用任何安全加密手段，直接对信息进行明文传输。黑客只要破解通讯传输协议，就可以直接读取其中所传输的数据信息，并任意进行篡改、屏蔽等操作。

对于物联网的通讯安全，首先需要加强网络通讯协议自身的安全防护。考虑到通讯协议本身就是由一行行代码所组成，针对代码的部分安全防护方法可以直接移植过来。也就是说，可以对通讯协议实施加密操作，采用多层密钥加密传输，密钥之间动态切换，提供更加安全的保证。通过白盒加密技术再对加密密钥进行安全性保护，防止密钥的泄漏和破解。对通讯协议代码实施高强度混淆，彻底“打乱”旧有程序逻辑

思路，极大增加黑客分析、破解、调试、Hook、Dump通讯协议的难度，甚至在超过破解性价比临界值时迫使黑客放弃入侵攻击。

其次，要对数据通讯传输管道里的数据流进行加密操作，杜绝明文传输。还要对流量里的数据进行安全过滤、安全认证，确保让正确的数据在通讯传输管道里流通。对设备指纹、时间戳信息、身份验证、消息完整性等多种维度的安全性校验，可以进一步保证数据传输的唯一性和安全性。另外要注意，在特殊物联网传输环境下，要考虑进行网络加速操作，避免数据通讯传输管道成为物联网体系正常运转的瓶颈所在。



物联融合的未来安全云平台

云平台能够对物联网终端所收集的数据信息进行综合、整理、分析、反馈等操作。针对云平台的安全产品、安全方案很多，也在逐渐成熟，不过对于物联网云平台而言，还需要加入移动安全这个维度的安全防御，例如需要移动威胁感知平台来完善云平台安全情报体系，通过SOC、M-SOC（Security Operation Center for Mobile）实现对物联网安全体系的整体管控，通过移动安全测评云平台实现对物联网云端应用、源码、服务器安全性的实时检验与监测。

如果说物联网终端相当于人的手脚、眼鼻口，网络通讯传输管道相当于人的四肢躯干，那么云端就等同于人的大脑，其安全重要性可见一斑。物联网云端保存着所有终端搜集上来的信息数据，以及据此分析获得的新数据信息。这些信息就犹如存放在仓库里的黄金珠宝，时刻诱惑着黑客发起攻击。云端一个小小的业务逻辑漏洞，就可能会给黑客攻击大开方便之门。

SOC并非一个新的概念，但在物联网时代，面对复杂的物联网安全体系，SOC的作用在变得愈加凸显。SOC作为安全体系的一个集中单元，会在整个组织和技术的高度处理各类安全问题。SOC能够将安全防御孤岛连接起来，从安全情报、安全产品、安全运维到安全服务，SOC可以使之不再割裂，提高整体安全防御效率，降低安全防御成本。SOC由于自身特点，使其所处位置只能是在云端层面：其或会依托于云计算平台，作为云平台内部的一个模块组件，或者单独以安全管理云平台的形式并列于云端之侧。

物联网与业务之间的结合达到了一个前所未有的高度，那么在物联网安全体系里，SOC将以业务为导向驱动，量化安全、展示安全、控制安全，实现安全管理技术化。通过SOC可以对物联网云端、终端、传输端进行逻辑层、物理层等多层面的安全检测，及时解决所发现的安全隐患，力争将危机消灭于萌芽之中。而借助SOC还能够洞悉物联网整体系统的安全态势，即时制定新安全防御策略，实施有效的安全防护动作，并实现对全网传统与新兴安全能力的整合，避免安全防护一盘散沙局面的出现。而M-SOC则能在物联网移动维度实现全生命周期的安全防护，有力补足了物联网安全体系可能出现的安全防护遗漏。

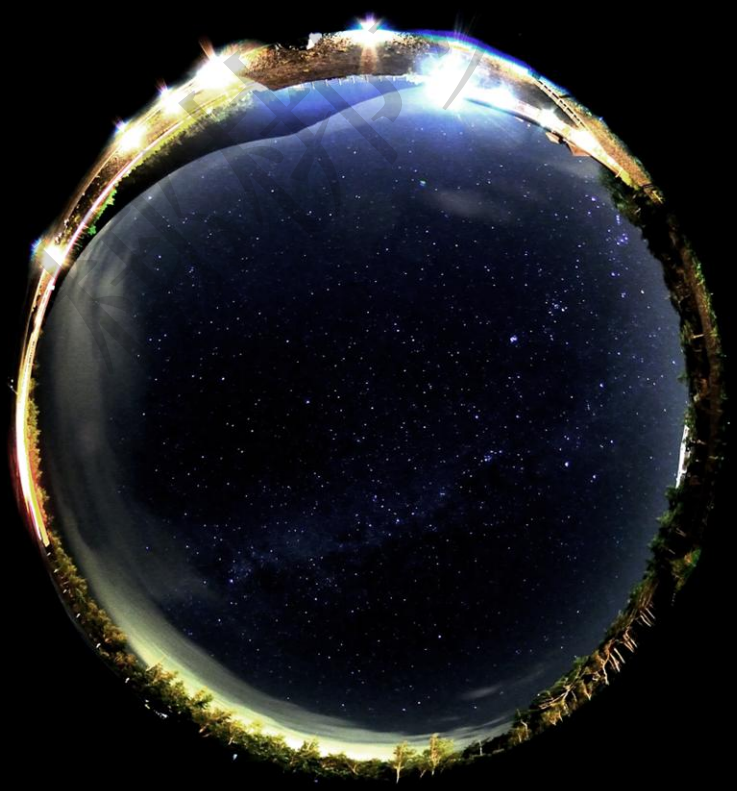
英国Newcastle大学的Leusse在其论文《Self managed security cell, a security model for the Internet of Things and Services》里提出了一种面向服务思想的安全架构，利用Identity Brokerage、Usage&Access Management、SOA（Service-Oriented Architecture） Security Analysis、SOA Security Autonomics等模块来构建具有自组织能力的安全物联网模型。

物联网的安全触角实在太为广阔，覆盖了众多领域维度。从大的方面考虑，需要各SOC能够实现耦合，进行安全防御联动，共享安全情报信息，整体把控物联网安全。往小的层面看，由微边界联合起来的众多物联网终端微点，要能够逐步实现矩阵化，从松散的个体成为组织化、智能自适应化的严谨统一整体。以集体的力量有效对抗有组织的恶意攻击。

在物联网时代，不同行业的云平台之间势必将互相连通起来，智慧城市可以说就是各类云平台的整合。而在云平台整合的背后，则联动着不同行业、不同领域物联网安全管控平台的整合，物联网安全体系内部各个环节的整合，物联网微观环境里各个单元、模组的整合。只有将一切松散元素锻造成严密的统一整体，才能将物联网安全清晰地呈现在人们面前。

如何度量安全？在物联网时代里，或将做到这一点。

加上全生态环境安全协同，可让物联网安全变得高度可控！



协同一致的物联网安全生态

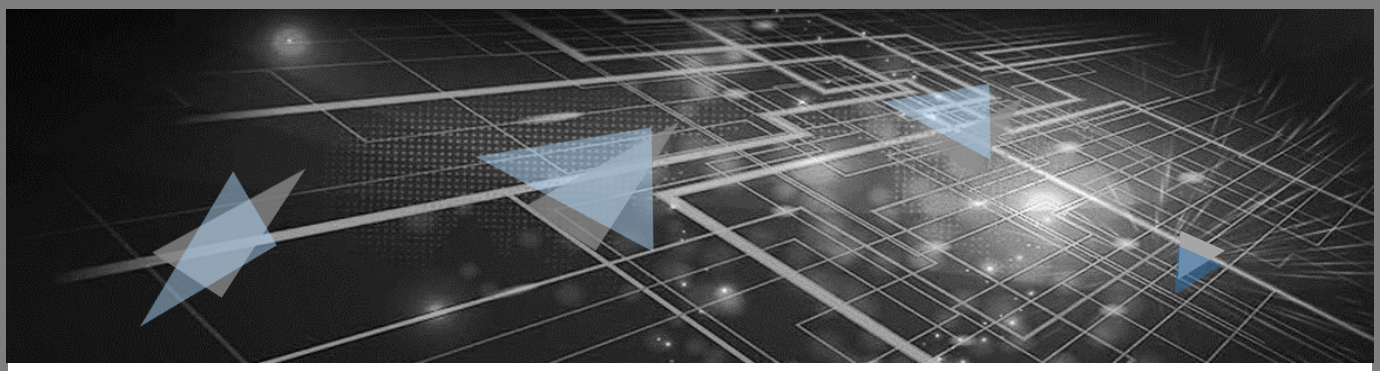
面对复杂多变的物联网体系，需要构筑足以将其完全容纳的物联网安全生态环境，这意味着，既需要“端管云”安全防御体系，还需要构建“大安全”生态系统。

物联网体系自身特点，决定了物联网安全必然会受到来自于上下游相关生态环境的影响。某国际著名企业所遭受的恶意攻击，就是由于一封从合作伙伴处发来的电子邮件所导致。在苹果Xcode Ghost病毒事件里，Xcode是由苹果制作的开发Mac OS和iOS应用程序最快捷、普遍的开发工具，恶意攻击者在Xcode中植入了恶意代码，当应用开发者下载并使用被感染的XCode开发程序时，恶意代码就会污染开发者端程序。这会使得即便未越狱的iOS用户从苹果官方App Store下载应用时也将面临各类安全威胁风险。

木桶定律对于物联网安全生态有着极为深刻的影响，最短的那块“安全防御木板”将不仅会降低物联网安全整体防御度，甚至可能引发严重的负面影响，导致一个或数个相关体系被恶意攻击所摧垮。在物联网时代下，哪怕一个普通人也需要作为一个安全防护单元，使得以该普通人为主导的物联网生态体系也能够拥有足够的安全防护能力。

同时还要注意，虽然传统安全防护产品已经无法有效应对新型恶意攻击，但并不意味着在物联网安全体系里就不再需要传统安全防护产品。恰恰相反的是，在物联网的网络层等维度中，传统安全防护产品依然起着不可或缺的作用。在物联网的安全生态环境里，一条坚固的传统安全防线极为重要。

单元普通人、传统网络安全防线、物联网应用层新型安全防线、上下游领域安全防线……对于物联网安全生态环境的构建永远都没有最大，而是要做到“恶意威胁有多大，安全就要比之再大上那么一点。”



可视可度量的物联网安全管理

人们一直希望能够度量世间万物，但对某些事物却始终无法找到有效的度量方法，安全就包括其中。

在计算机时代，人们可以统计系统被感染了多少病毒，但却无法准确衡量病毒对系统造成了多大的损坏。近几年人们所热议的安全可视化，其背后也是在探寻可以对安全进行衡量的方法。人们希望能够看到“不可见的安全”，人们更希望能够对安全体系的强壮程度进行丈量。人们需要更为明确地知晓自己所构建的安全防线是合格、优秀还是满分，或者是处于不及格之下，需要对其中部分环节进行提升。

物联网世界里的安全更需要做到可度量，并据此找寻、设立适用于各领域的安全基线，二者相结合精准掌控物联网安全。

实际上，随着安全防护能力的细微化，度量安全的方法也在逐渐清晰起来。以移动应用安全为例，移动应用自身的源代码、库文件、密钥、软键盘、启动界面、交互短信、通讯协议等等都是其主要的防护节点。那么最为简单的移动应用安全度量就可以是：依据各个节点是否实施了安全防护、采用了怎样强度的安全防护技术进行评分，综合得出安全防御度分数。进而根据不同行业、不同业务对于防御节点数量及强度需求的不同，设立各自的安全基线。金融行业对于安全性要求很高，那么可能其安全基线分数要达到90分以上才算及格，超过120分才算优良。

安全度量与安全基线这两大要素，将使物联网安全变得高度可控。

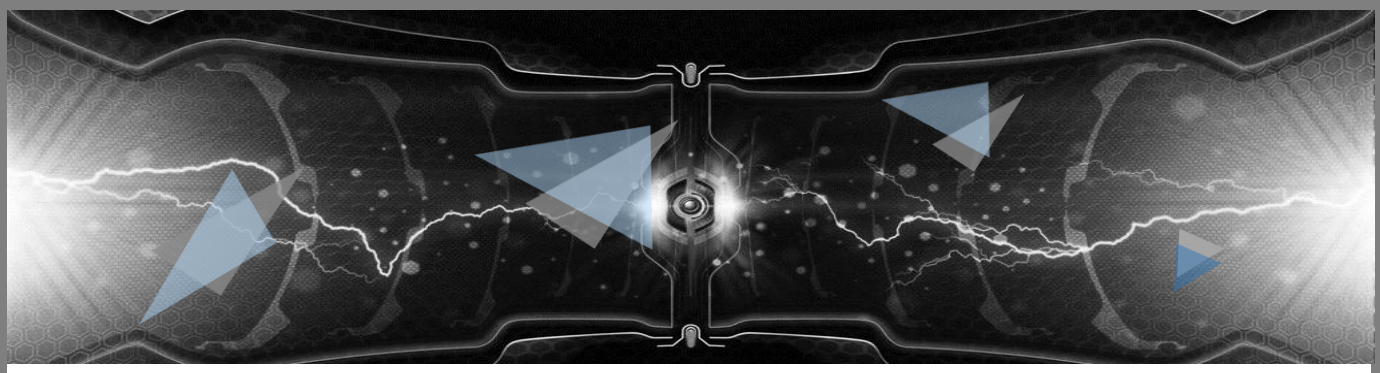
网络摄像头很小，却能瞬间让数亿人“下线”断网；

老司机控制下的智能汽车，竟然还会突然“发疯”到处乱撞；

温馨的智能家庭，虚拟空间中的“窃贼”早已悄然潜入。

这是物联网世界里已经或者正在发生的真实事件！这一切都是黑客以及恶意攻击者们捣的鬼！

好消息是，安全研究人员已经想到了一些解决方法，供您参考。



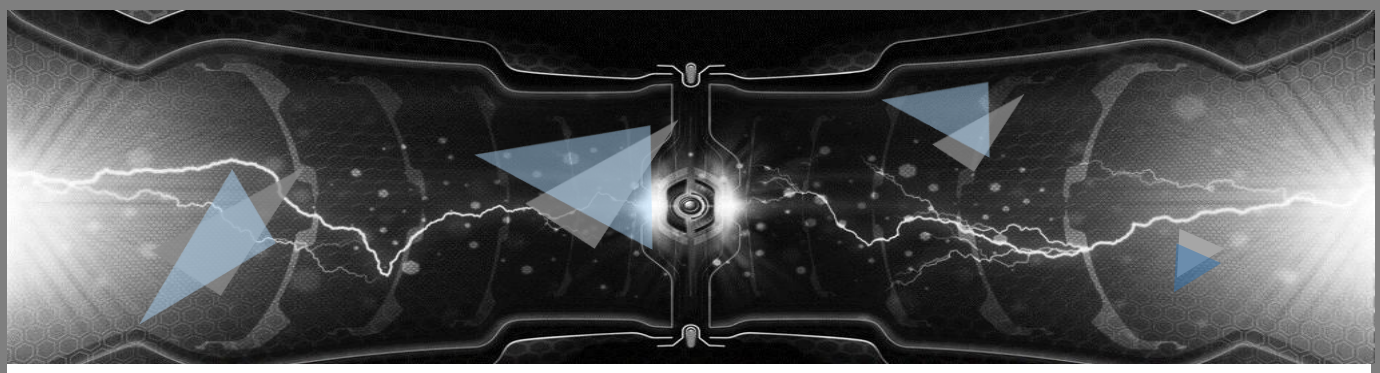
典型物联网环境安全防御

（一）网络摄像头背后的物联网安全危机

今年所发生的大规模物联网DDoS测试攻击，导致了美国东部互联网全部“下线”。而其罪魁祸首之一竟然是国内某安防视频产品方案和技术提供商所生产的摄像模组，该摄像模组被许多网络摄像头、DVR厂家采用，并于美国大量销售。该公司部分早期摄像模组产品的密码被写入到固件里，且很难进行修改。黑客发现了这一可乘之机，通过默认密码打开了大门，控制其成为了物联网DDoS攻击的肉鸡。如此不经意的一个问题，竟然就让小小的网络摄像头发挥出如此“巨大的作用”！

由此可见，物联网繁多的各类终端里一个不起眼的小毛病一旦被黑客挖掘出来，加乘上终端设备庞大的个体数量，所将爆发出来的破坏力不容小觑。

而在安全研究人员的眼里，物联网终端安全防护的办法其实有很多。举例来说，对于可穿戴智能设备安全防护的关键节点包括（不限于）：防止对其内部程序代码的静态分析与运行时的动态调试；加密敏感存储数据，在运行时解密；保护可穿戴设备SDK，避免拦截、篡改数据；加固应用程序，拒绝未经授权的更改；防止逆向工程、窃取知识产权，避免盗版侵权；实现一机一密，并利用白盒技术深度保护密码等等。



典型物联网环境安全防御

（二）智能网联车不可变成“智能撞翻车”

自从特斯拉惊艳亮相之后，人们才发现原来汽车的世界还可以是这样，原来科幻电影里炫酷的未来交通工具也能够来到我们的身边。而其中最为兴奋的竟然是网络安全世界里的黑客们，各种花样的玩转特斯拉。

但从智能网联车自身角度来看安全能够发现，T-BOX、IVI、OBD、USB、充电接口、GPS、摄像头等更多的攻击入口，动力系统、转向系统、制动系统、车身控制系统、仪表盘等更多的被攻击点在越来越多地暴露在人们视野里。智能汽车与外部的每个接口都可能被利用，每个控制单元都可能被攻击。

再从智能网联车的生态环境来看，与智能汽车有信息交互的外部组件如果被入侵，都可能引发智能汽车的信息安全事件、交通安全事故。例如智能汽车的充电桩、行车记录、智能标示牌等等一旦被恶意攻击，“无人驾驶”失控将更为“频繁”。

无需认证、明文传输、通信流程伪造……智能网联车的生态环境中面临的潜在安全风险几乎无处不在。现实生活中，已经有厂商因为各类信息安全问题，开始召回存在安全隐患的智能汽车。

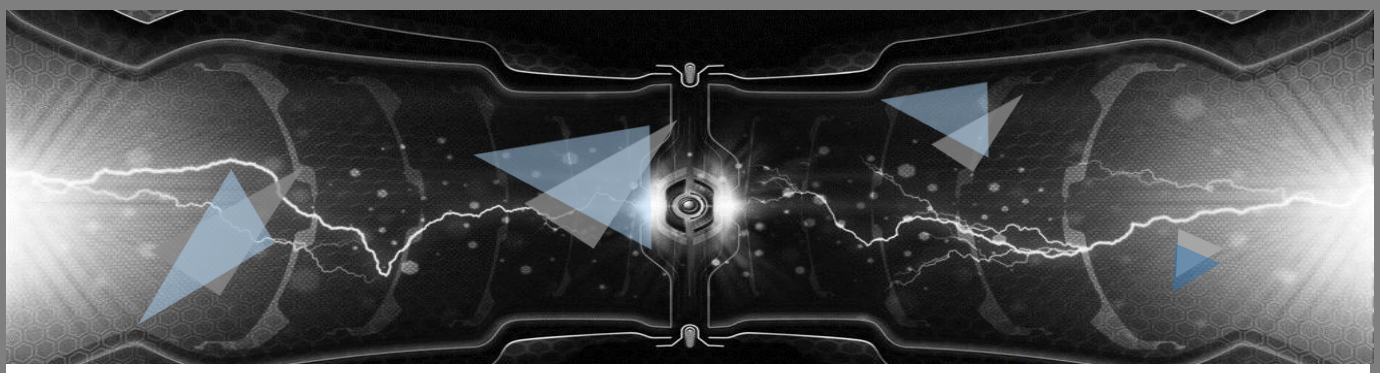
车联网是物联网的重要分支，作为车联网核心要素之一的智能汽车所暴露出来的安全问题，将直接影响到人们的生命安全。那么对于智能网联车的安全防御要能够做到：

1、从内到外：从车内部到整个外部生态环境安全；

2、从小到大：从芯片安全到云安全，对应各点提供保护；

3、从始到终：从安全设计到安全运营。

也就是要实现，从车内到外部的生态环境、从微小的芯片到云端平台、从智能汽车诞生之前到其生命的终结，全维度、全生命周期的安全能力覆盖。

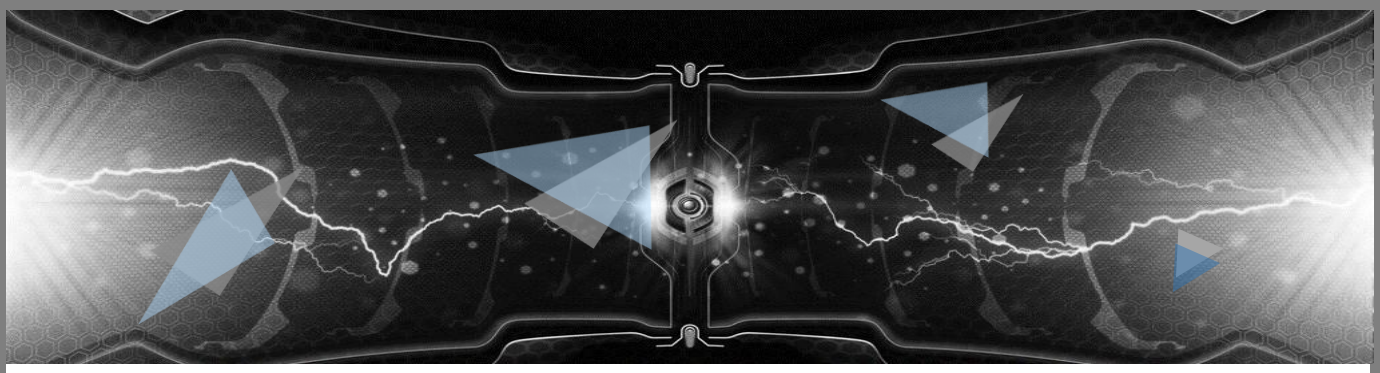


对于智能网联车的安全防御可以参考如下原则：

1、架构全面性：采用端管云安全架构体系，考虑整个生态的安全需求；

2、方案综合性：层次化、多样性的特点将更为突出，应根据风险分析合理实施纵深防护方案，部署适合的安全防护产品；

3、技术创新性：随着智能化、网联化与电动化的进一步发展，会出现更多新的攻击手段，需要超越原有理念，采纳新技术防护。



典型物联网环境安全防御

（三）家庭里的那朵安全智能云

现在许多人的手上会有三部移动设备：智能手机、智能手表（智能手环）、平板电脑。而当人们回到家里后，需要联网的智能设备会增加为智能门锁、智能电视、智能空调、智能冰箱、智能洗衣机等等。

物联网另外一个重要分支——智能家庭网络的雏形开始显露出来。

然而，绝大部分智能家居产品在设计、生产过程中都没有将安全性考虑进去，黑客对于智能家居产品的破解几乎是手到擒来。去年就频繁爆出各类智能家居产品存在安全漏洞、安全隐患，某国外品牌智能电视会将语音搜索功能产生的信息数据直接明文发送到网络，黑客通过网络嗅探就可以窃取到这些没有进行加密的用户信息。

那么对于智能家庭网络里的各类终端——智能家电的安全防护，要注意防止绕过、屏蔽身份认证机制；要防止通过互联网对智能家电进行侵入式的恶意控制；还需要加壳保护智能家电的控制应用App，增强App安全度，避免其成为整体防御架构中的薄弱节点。

扩展到智能家庭网络，其安全防御策略要能够阻止未经授权对智能家居设备的开启、关闭等控制，要阻止智能家居设备控制电子密钥的非授权发送。更为深入则可以考虑通过白盒密码技术对存储在本地的电子密钥/证书进行保护，并保护通讯协议及数据，防止针对性的音频、视频等信息数据被窃取。

结束语

物联网的一个重要应用场景就是智慧城市，而智慧城市的安全防护则包含了城市基础通讯、能源、气候、交通、教育、视频、新闻、医疗、行政等诸多领域。相信在不久以后的物联网时代，在更多场景里都将看到物联网的身影。

而无论物联网如何变化，其“终端——传输管道——云端”这一本质架构形式将不会发生改变。所以，对于物联网的安全防御动作必须要紧扣其架构本质，保护好智能终端、通讯数据、云服务器等环节，并将安全能力细微化、极大化、整体化，借助安全度量与安全基线清晰物联网安全。

公司介绍

梆梆安全成立于 2010 年，是全球专业的移动应用安全服务提供商，运用领先的技术提供专业可靠的服务，为全球的政府、企业、开发者和消费者打造安全、稳固、可信的移动应用生态环境，让每个人都能自由地创造、分享和使用移动信息。

梆梆安全不仅提供APP安全保护、威胁情报、事前/事后应急响应等服务，同时面向行业提供全套安全方案，针对业务定向威胁提供贯穿生命周期的纵深防御体系。今天，梆梆安全的使命是“保护智能生活”，并已经推出车联网、智能家居等相关解决方案。在将安全能力渗透到各类终端的同时，梆梆安全还打造出了把安全能力延伸至传输端以及云端的泛在安全云防护系统。面对快速发展的人工智能，梆梆安全更是前瞻性地提出认知安全理念。

到目前为止，梆梆安全已经为7万家注册企业及开发者的超过70万个移动应用提供移动应用安全服务，这些应用已经累计安装在7亿个移动终端上。梆梆安全的企业用户遍及金融、互联网、物联网、政府、企业等各大行业，覆盖亚洲、欧洲及北美等主要市场。